

1. 추출 데이터

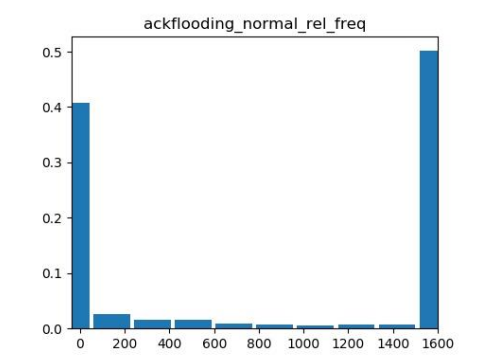
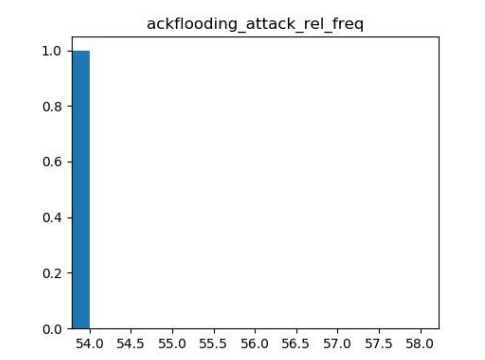
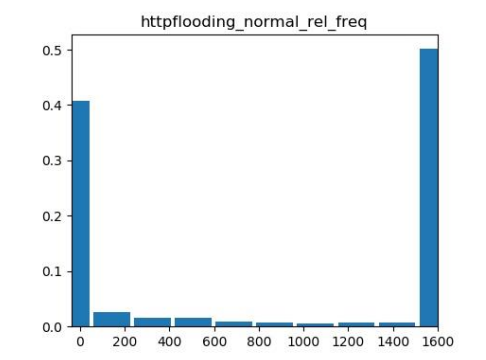
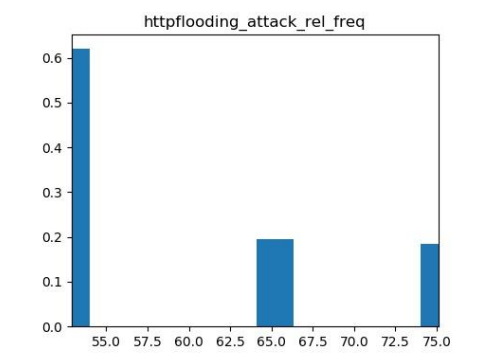
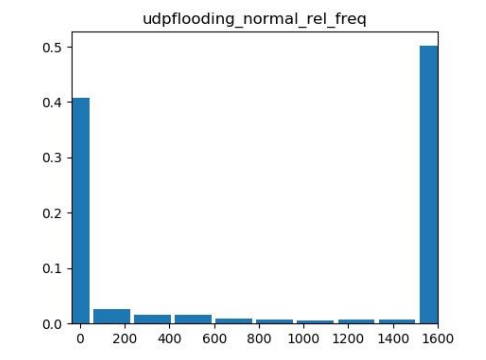
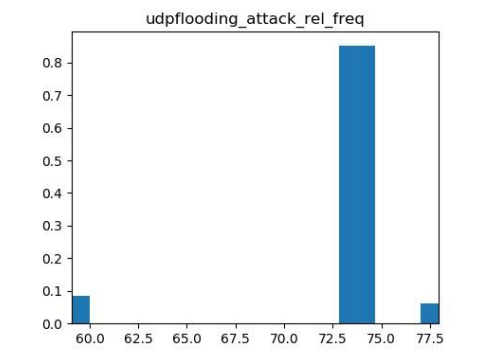
srcIP	dstIP	srcPort	dstPort	protocol	seq	ack	flags	method	uriLen	status	host	user-agent	cookiesLen	len	class
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							66	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1511	FALSE
192.168.0.239	255.255.250.1900	57857	1900	UDP				ETC			239.255.255.250:1900			179	FALSE
192.168.0.192	168.0.192	1900	57857	UDP				response		200				445	FALSE
192.168.0.239	255.255.250.1900	57857	1900	UDP				ETC			239.255.255.250:1900			179	FALSE
192.168.0.239	255.255.250.1900	57857	1900	UDP				ETC			239.255.255.250:1900			179	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							78	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							78	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1511	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							78	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							78	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							78	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							66	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							66	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							66	FALSE
104.118.13.192	192.168.0.113	443	43238	TCP	3.4E+09	1.65E+09	PSH,ACK							1507	FALSE
192.168.0.104	192.168.0.113	43238	443	TCP	1.65E+09	3.4E+09	ACK							66	FALSE
192.168.0.239	255.255.250.1900	57857	1900	UDP				ETC			239.255.255.250:1900			179	FALSE

- srcIP: 발신지 IP
- dstIP: 수신지 IP
- srcPort: 발신지 Port
- dstPort: 수신지 Port
- Protocol: 프로토콜(UDP, TCP)
 - 압도적으로 UDP, TCP 가 많은 수로 존재하기에 이외의 protocol 들은 제외
- seq: seq
- ack: ack
- flag: ack, psh, fin
- method: GET, POST, response, ETC
- uriLen: URI 의 길이
- status: status
- host: host
- user-agent: User-Agent
- cookiesLen: cookie 의 길이
- len: 패킷의 길이
- class: True=공격패킷, False=정상패킷. 정상, UDP Flooding, Ack Flooding, Http Flooding 으로 수정 예정

2. 공격 유형별, 정상, 공격 분류에 따른 패킷 길이 평균, 표준편차, 개수

Type	normal			Attack			normal + attack		
	len_mean	len_std	count	len_mean	len_std	count	len_mean	len_std	count
ackflooding	829.886	687.196	237830	54	0.029	75632	642.68	684.4717	313462
httpflooding	829.886	687.196	237830	60.012	8.082	10464	797.441	690.1201	248294
udpflooding	829.886	687.196	237830	73.002	4.018	949284	224.639	431.7409	1187114
total	829.886	687.196	713490	71.483	6.421	1035380	380.89	575.8535	1748870

3. 공격 유형별, 정상, 공격 분류에 따른 패킷 길이의 상대적 빈도수

Type	Normal	attack
ackflooding		
httpflooding		
udpflooding		

total

